REMARKS/ARGUMENTS

These remarks are made in response to the Office Action of January 31, 2005 (Office Action). As this response is timely filed within the 3-month shortened statutory period, no fee is believed due.

In the Detailed Action, the Examiner has rejected claims 1-40 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,707,889 to Saylor, *et al.* (Saylor) in view of U.S. Patent No. 6,681,327 to Jardin (Jardin).

Prior to addressing the rejections on the art, a brief review of the Applicants' invention is in order. The Applicants' claimed and disclosed subject matter teaches a secure means for conveying VoiceXML content between a network device and a Voice Browser. Specifically, the Voice Browser can authentic itself to the network element. Subsequently, a shared secret can be negotiated between the Voice Browser and the network device. The network device can encrypt VoiceXML content using the shared secret as an encryption key and convey the encrypted content to the Voice Browser. The Voice Browser can decrypt the content using the shared secret as a decryption key. The claimed invention provides a secure data conduit between the VoiceXML server and the network element.

Establishing a secure conduit or pipeline for conveying information ensures that outsides entities cannot obtain data as it is being transferred from point B (voice browser) of the conduit to point C (network element) of the conduit. Typically, an additional interaction occurs between a telephone user and the voice browser over a telephone line. This connection can be considered a new information conduit from point A (user) to point B (voice browser), which is generally a speech communication circuit between a user and an interactive voice response (IVR) system.

Saylor discloses a content retrieval system that permits a user of a voice response system (VNAP) to selectively access voice enabled Web pages from a voice server by providing a voice response system with a key (VCode) associated with the desired Web page. The purpose of Saylor is to provide a content access system linked to the VCode registration system so that users can obtain VCoded data via a telephone line. Saylor teaches that a user may have to provide authorization information before accessing VCode information. Saylor provides no teachings pertaining to secure data conduits or transmission channels.

Jardin teaches a method and a system for speeding up secure client-server transactions by using a plurality of servers to assure that a server is available to transmit information whenever a client is ready to receive the information. Jardin teaches establishing a secure connection between a client and a broker. Jardin makes no specific reference regarding voice browsers.

Referring to claim 1, Applicants claim the steps of:

transmitting a request to the network device to establish a secured communication session between the Voice Browser and the network device;

authenticating the network device;

subsequent to said authentication, negotiating a shared secret between the network device and the Voice Browser;

encrypting the VoiceXML-based Web content using said shared secret as an encryption key;

exchanging the encrypted VoiceXML-based Web content between the network device and the Voice Browser; and,

decrypting the VoiceXML-based Web content using said shared secret as a decryption key.

Saylor is cited for teaching establishing a secure communication between a Voice browser and a server. Applicants, however, assert that Saylor provides no such teaching, but instead teaches a user authentication method.

By a user authentication method, Applicants mean that Saylor teaches that a user (A) must authenticate itself to a server (B), which can include a voice browser, before being authorized to receive data (X), controlled by the server. This authentication is discussed in cited column 10, lines 17-40 and specifically at column 10, lines 35-37. Notably, data X can be obtained from a network element (C). Hence, data X is conveyed from C to B to A. Saylor fails to contemplate that the data conduit C to B over which data X is conveyed is a secured and/or encrypted data conduit, as explicitly claimed by the Applicants.

To prove that Saylor lacks such a teaching, Applicants shall briefly analyze the cited portions of Saylor, which are alleged to contain teachings regarding secure data conduits.

(1) column 10, lines 17-40 – details a user authentication system for accessing data. (i.e. authorizing person A to access data X)

(2) column 26, lines 45-63 – shows the V-code registration system but makes no comments about a secure data conduit (NOTE: from figure 7, a secure data conduit between a voice browser and a network element would be the conduit between web interface system 86 and voice server 43)

(3) column 2, lines 1-25 – provides no reference of a secure data conduit

(4) column 11, lines 24-36 – discusses caller authorization to access data. Caller authorization can be based upon voice print identification and/or a password input (i.e., authorizing person A to access data X).

(5) column 17, lines 16-39 – discusses configuring a user authentication level.

Consequently, Saylor fails to teach the establishing of a secure data conduit (from B to C) over which data can be conveyed, as claimed by the Applicants.

In contrast, Jardin does teach a secure data conduit between a client and server, specifically between a client and a broker. Jardin fails, however, to teach or suggest that a secure data channel can be established between a voice browser and a network element.

As noted in the background (page 1, line 18 to page 2, line 18), SSL has been typically integrated directly with selected underlying application protocols. Further, SSL compliant **visual** Web Browsers existed at the time of the Applicants' invention. As noted between page 3, lines 16 and page 4, line 21 of the background, at the time of the Applicants' invention, SSL had not been integrated with Voice Browsers. Neither Saylor, Jardin, nor combinations thereof provide such teachings or suggestions to integrate SSL (or other secure data conveyance conduit) with Voice Browsers, as claimed by the Applicants herein.

In terms of establishing a secure channel of communication, Voice Browsers are very different from Web browsers, which the Applicants shall take a moment to elaborate upon. In a Web browser, a user logs onto their computer (computer A) and accesses a network element (computer B). The user can load public keys, certificates, and other shared secret data on computer A. The data conduit between computer A and B is secured for a transaction, such as a transaction when a Web browser changes from "http" to "https" to indicate that a secure data transmission channel exists. Sensitive information, such as a credit card number, can be conveyed over this secure data channel. Conventional teachings provide various mechanisms for establishing the secure data channel between A and B, when A is a computer having a visual Web browser being used to access data from Web site (network element) B.

When a voice browser is utilized, a caller calls from a telephone (point A) to an interactive voice response system (IVR) having voice browsing capabilities (point B). The voice browser (B) can convey information between a network element (C). In this scenario, the user A does not control or "own" the voice browser (B) which is used by numerous telephone users. That is, according to conventional teachings, the voice browser does not have shared secret information that can be used to establish a secure data conduit with a network element.

Accordingly, before the Applicant's claimed invention, when a user provides their credit card number to an IVR that in turn provides it to a network element, an intruder could intercept the message between points B and C and acquire the user's credit card number. Neither Saylor nor Jardin teach nor suggest a means to securely convey the credit card information between points B and C, which is claimed by the Applicants, so as to prevent interception of data between these points.

In summary, neither Saylor, Jardin, nor combinations thereof explicitly or implicitly teach each claimed limitation of the Applicants invention. Specifically, the limitation of a secure data conduit or a secure communication session between a voice browser and a network device is not explicitly or implicitly taught. Consequently, the 35 U.S.C. § 103(a) rejections to claims 1-40 should be withdrawn, which action is respectfully requested.

Although Applicants claims should now be in an allowable condition, Applicants shall take a moment to point out a few additional differences between the claimed invention and the referenced art.

Regarding claims 8 and 28, the authentication process taught by Saylor relates to authenticating a user to access data, not authenticating a voice browser to establish a secure data channel.

Regarding claims 9 and 10, Saylor discloses that a user can configure an authentication level (column 17, lines 16-31) or that a content provider can provide a

data authentication level (column 22, lines 39-45). These teachings pertain to user authentication not to secure data transmission over a secure data conduit.

In light of the above, Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned (direct line 954-759-8937) if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: 31 March 2005

Gregory A. Nelson, Registration No. 30,577
Brian K. Buchheit, Registration No. 52,667
AKERMAN SENTERFITT
Customer No. 40987
Post Office Box 3188
West Palm Beach, FL 33402-3188
Telephone: (561) 653-5000